Bijlage 6
Beveiliging

IWR2021|Werkplek-hardware|Diensten

ICT Werkomgeving Rijk

Status:	versie 1.0
Referentie:	IUC 202006119-5

Inhoud

1 Inleiding

Op het gebied van informatiebeveiliging van de informatievoorziening dienen de Hoofdopdrachtgever en de Deelnemers zich te houden aan vastgestelde regels voor de Rijksoverheid. De regels over informatiebeveiliging voor de Rijksoverheid zijn onder meer terug te vinden in:

- Beveiligingsvoorschrift Rijksdienst (BVR)[1];
- Baseline Informatiebeveiliging Overheid (BIO)[1];
- Voorschrift Informatiebeveiliging Rijksdienst (VIR)[1];
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-bi)[1];
- de Algemene Verordening Gegevensbescherming (AVG)[1];
- het Algemeen Rijksambtenarenreglement (Wnra)[1].

De Prestatie die Opdrachtnemer levert is integraal onderdeel van de informatievoorziening waar de rijksdienst gebruik van maakt. Dit betekent dat de Diensten van Opdrachtnemer niet strijdig mogen zijn met het beveiligingsbeleid van Hoofdopdrachtgever en/of Deelnemers.

De regels op het gebied van informatiebeveiliging die gelden voor de Rijksoverheid zijn gebaseerd op de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 normen. Opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.

In deze Bijlage zijn de beveiligingsaspecten die op deze Raamovereenkomst van toepassing zijn opgenomen[2]. Deze beveiligingsaspecten zijn onder te verdelen in:

- beveiligingseisen die gesteld worden aan Personeel dat door de Opdrachtnemer wordt ingezet voor het uitvoeren van alle voorkomende werkzaamheden zoals deze zijn onderkend;
- beveiligingseisen die gesteld worden aan de (levering van) Diensten;
- beveiligingseisen rondom de uitvoering van de Diensten.

In het Dossier afspraken en procedures (DAP) tussen de Opdrachtnemer en de Deelnemer worden alle specifieke beveiligingsafspraken tussen de Opdrachtnemer en de Deelnemer vastgelegd.

Wet- en regelgeving is niet statisch. Opdrachtnemer zal zich conformeren aan de actuele wet- en regelgeving. Uitgangspunt hierbij is dat de scope en reikwijdte van eventuele opvolgers van bestaande wet- en regelgeving niet wezenlijk wijzigen.

[1] Zie hoofdstuk 5 Bronvermeldingen voor de link naar het document

[2] Zie bijlage 2 'Specificatie van de Prestatie' Eisen 13.1

2 Eisen aan Personeel van Opdrachtnemer

2.1 Personeel

De Opdrachtnemer zet Personeel in voor het uitvoeren van alle voorkomende werkzaamheden zoals deze zijn onderkend. Onder Personeel van de Opdrachtnemer wordt verstaan medewerkers van de Opdrachtnemer die worden ingezet. Een niet uitputtende opsomming van werkzaamheden die te onderkennen zijn, is:

- werkzaamheden door personen die deel uitmaken van het accountteam;
- werkzaamheden door personen die betrokken zijn bij de Installatie;
- werkzaamheden door personen die betrokken zijn bij de uitvoering van de Diensten;
- werkzaamheden door personen die de incidentafhandeling uitvoeren.

Op verzoek van de Deelnemer dient Personeel van de Opdrachtnemer een VOG te overleggen die niet ouder is dan twaalf maanden. De kosten voor dit document zijn voor rekening van de Opdrachtnemer.

De Deelnemer kan eisen dat Personeel van of namens de Opdrachtnemer een geheimhoudingsverklaring ondertekent. De Deelnemer kan aanvullende screening eisen voor het Personeel dat door de Opdrachtnemer wordt ingezet. Indien de Deelnemer aanvullende screening of aanvullende geheimhouding eist, dienen bijbehorende voorwaarden en condities tussen de Deelnemer en de Opdrachtnemer vastgelegd te worden in de beveiligingsparagraaf van het Dossier afspraken en procedures (DAP). De kosten voor deze aanvullende screening komen voor rekening van de Deelnemer.

Personeel van Opdrachtnemer dat niet aan de gestelde beveiligingsvoorwaarden voldoet kan in beginsel niet door Opdrachtnemer worden ingezet. Hier kan alleen van worden afgeweken wanneer Hoofdopdrachtgever en/of Deelnemer hiervoor aan de Opdrachtnemer een tijdelijke ontheffing verleend.

Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren, vastleggen en uitvoeren van taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging voor de Prestatie en dient naar het Personeel van de Opdrachtnemer te communiceren dat:
1. deze van kracht blijven na beëindiging of wijziging van het dienstverband;
2. deze ten uitvoer moeten worden gebracht.

2.2 Toegang tot Locatie

Bij het betreden van een Locatie dient een medewerker van de Opdrachtnemer zich altijd te kunnen legitimeren met een wettelijk geldig legitimatiebewijs. Op de website van de Rijksoverheid is op de pagina identificatieplicht opgenomen welke identiteitsbewijzen voldoen[3]. Personeel van de Opdrachtnemer zal handelen conform de op de Locatie geldende huisregels, wettelijke bepalingen en aanwijzingen van de Deelnemer.

[3] Zie hoofdstuk 5 Bronvermeldingen voor de link.

De Deelnemers kunnen aanvullend eisen dat bij het betreden van de Locatie legitimatie plaatsvindt in combinatie met een kopie van de VOG van desbetreffende medewerkers van de Opdrachtnemer, alsmede een kopie van de door die persoon ondertekende geheimhoudingsverklaring. De Deelnemers zullen dit vooraf bekendmaken en vastleggen in het Dossier afspraken en procedures (DAP) tussen de Deelnemer en de Opdrachtnemer.

Indien de Deelnemer van mening is dat medewerkers die door de Opdrachtnemer ingezet worden op Locatie begeleid dienen te worden, zal de Deelnemer zorgdragen voor deze begeleiding.

3 Beveiliging bij Diensten

Beveiliging bij Producten en Diensten omvat de volgende aandachtsgebieden:
- beveiliging Producten, Diensten en Programmatuur algemeen;
  - innemen van Producten;
  - reparatie op locatie;
  - penetratietest;
  - toegang tot het centraal beheerplatform;
- remote beheer;
- logging van gegevens;
- authenticatie;
- beveiligingsinstellingen Product en Programmatuur;
- Beveiliging van transport.

In te zetten beveiligingsmaatregelen worden steeds in samenspraak met de Deelnemers vastgesteld.

3.1 Beveiliging Producten en Programmatuur algemeen

De Opdrachtnemer is voor zover binnen de te leveren Dienst(en) van toepassing verantwoordelijk voor de adequate beveiliging van de Producten en Programmatuur. Onder adequate beveiliging is onder andere inbegrepen: het kunnen aanmaken en verwijderen van accounts, een autorisatiemodel voor deze accounts, het gebruik van geëncrypte wachtwoorden en indien van toepassing maatregelen tegen malware, mogelijkheden voor back-ups en mogelijkheden voor logging, het toepassen van versleutelde protocollen en bescherming bij uitwisseling van elektronische berichten.

Wijzigingen welke de beveiliging kunnen aantasten worden voorafgaand met de Deelnemer besproken, waarbij de risico's worden benoemd en eventuele maatregelen worden geadviseerd. Alle beveiligingsrisico's worden door de Opdrachtnemer direct bij constatering kenbaar gemaakt bij de Deelnemer/System integrator, ook als het de instellingen of specifieke configuratie van een Deelnemer betreft. Tevens doet Opdrachtnemer voorstellen om de beveiliging te verbeteren.

Indien Opdrachtnemer voor het leveren van een Product of Dienst gebruik maakt van een Onderaannemer, dan gelden voor de Onderaannemer dezelfde beveiligingseisen als voor hemzelf.

In alle gevallen blijft Opdrachtnemer verantwoordelijk voor borging bij de Onderaannemer van de met de Deelnemer gemaakte afspraken.

3.2 Innemen Producten

In bepaalde gevallen, bijvoorbeeld in verband met het kunnen voldoen aan zijn onderhoudsverplichtingen, zal de Opdrachtnemer overgaan tot het innemen van Producten. Een Product mag echter niet zonder voorafgaande toestemming van de Deelnemer van de Locatie worden meegenomen. Daarnaast dienen eventueel aanwezige gegevensdragers op een vooraf met de Deelnemer overeengekomen en verantwoorde wijze te worden behandeld.

Uit beveiligingsoverwegingen kan de Deelnemer aanvullende eisen stellen aan de gegevensdragers (HDU's, Flash-memory, etc.) die zich bevinden in het in te nemen Product of delen van het Product. Voorbeelden van deze aanvullende eisen zijn hieronder opgenomen.

- Aanwezige gegevensdragers dienen uit het Product te worden verwijderd door de Opdrachtnemer indien het Product de Locatie verlaat. De verwijdering vindt plaats op Locatie van de Deelnemer en de gegevensdragers blijven achter op Locatie van de Deelnemer.
- Gegevens op een te vernietigen gegevensdrager (met uitzondering van besturingssoftware) zijn, indien de technische staat van de gegevensdrager dit mogelijk maakt, op een door de Deelnemer aangegeven wijze overschreven of gewist (Permanent Image Overwrite) alvorens de gegevensdrager een Locatie verlaat.
- De Opdrachtnemer verstrekt binnen tien Werkdagen nadat de gegevensdrager is ingenomen een certificaat aan de Deelnemer waaruit onomstotelijk blijkt dat de Opdrachtnemer de gegevensdagers heeft vernietigd.
- De Opdrachtnemer verstrekt binnen tien Werkdagen nadat het Product is ingenomen een certificaat aan de Deelnemer waaruit onomstotelijk blijkt dat de gegevens op de gegevensdragers op de door de Deelnemer aangegeven wijze zijn gewist, dan wel overschreven.

Indien Producten die voorzien zijn van gegevensdragers de Locatie van de Deelnemer verlaten, dient de Opdrachtnemer een proces-verbaal op te maken waarin ten minste de volgende gegevens zijn opgenomen:

- datum en tijdstip verwijdering resp. wissen/overschrijven;
- NAW-gegevens van de Locatie;
- type- een serienummer van de apparatuur;
- serienummer(s) van de verwijderde resp. gewiste/overschreven gegevensdrager(s);
- naam en handtekening van het betrokken Personeel van de Opdrachtnemer, die de gegevensdrager(s) heeft verwijderd resp. heeft gewist/overschreven;
- naam en handtekening plaatselijke Interne Beveiliging Functionaris (IBF) resp. medewerker van de Deelnemer, die bij de verwijdering resp. het wissen/overschrijven van de gegevensdrager(s) aanwezig was.

3.3 Securitytesten

Het online portaal van de Opdrachtnemer wordt jaarlijks door Opdrachtnemer getest op kwetsbaarheden door middel van securitytesten (bijvoorbeeld whitebox penetratietesten) en de uitkomsten van deze securitytesten worden aan CCM ter beschikking gesteld.

Een Deelnemer kan ook voor eigen rekening een partij selecteren voor uitvoering van deze securitytesten. Deze testen kunnen onder andere bestaan uit:

- beoordeling van de opzet, bestaan en werking van informatiebeveiligingsmaatregelen;
- vormen van een oordeel over de betrouwbaarheid (beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid) door middel van een security assessment.

De Opdrachtnemer dient de hiervoor vereiste medewerking te verlenen en de bevindingen op te volgen indien deze zodanig zijn dat dit leidt tot onvoldoende beveiligde (delen van het) online portaal. Bevindingen die door Deelnemer gewenst worden, maar boven het overeengekomen beveiligingsniveau liggen komen voor rekening van de Deelnemer.

3.4 Afhandeling van Incidenten en Onderhoud op Locatie

Uit beveiligingsoverwegingen kan de Deelnemer eisen dat afhandeling van Incidenten en Onderhoud van Producten met een datadrager op de Locatie van een Deelnemer plaatsvindt. Indien de Deelnemer Onderhoud op Locatie eist, dient de Deelnemer de Opdrachtnemer hierin adequaat te faciliteren.

3.5 Penetratietest

Een Deelnemer kan voor eigen rekening een partij selecteren voor uitvoering van een penetratietest (PENtest) op het online portaal van de Opdrachtnemer. Deze test bestaat onder andere uit:

- beoordeling van de opzet, bestaan en werking;
- vormen van een oordeel over de betrouwbaarheid (beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid) door middel van een security assessment.

De Opdrachtnemer dient de hiervoor vereiste medewerking te verlenen en de bevindingen op te volgen indien deze zodanig zijn dat dit leidt tot onvoldoende beveiligde (delen van de) het online portaal. Bevindingen die door Deelnemer gewenst worden maar boven het niveau van Departementaal VERTROUWELIJK liggen, zullen voor rekening van de Deelnemer komen.

3.6 Remote beheer

Onder remote beheer wordt verstaan het verrichten van handelingen ten behoeve van het (technisch) beheer dat plaatsvindt vanuit een locatie die gelegen is buiten de infrastructuur van de Deelnemer. Uitgangspunt is dat het remote beheer niet wordt toegestaan, tenzij de Deelnemer hiervoor schriftelijk toestemming heeft gegeven. Indien de Deelnemer remote beheer toestaat, gaat Opdrachtnemer akkoord met de hieronder genoemde en de eventueel aanvullende voorwaarden die door de Deelnemer kunnen worden gesteld.

Voor remote beheer geldt dat dit door de Deelnemer uitschakelbaar is. Remote beheer is uitsluitend toegestaan via een beveiligde verbinding, waarbij de wachtwoorden eveneens beveiligd zijn tijdens het transport. De toegang kan zowel webbased als via een speciale voorziening zijn. Hierbij geldt o.a.:

- encryptie: AES 256 of beter;
- hash algoritme: SHA2 of beter;
- beveiligingscertificaten: X.509 versie 3 of beter;
- beveiliging van webverkeer: HTTPS of beter;
- beveiliging van verbindingen: TLS 1.2 of de logische opvolger.

Tevens geldt dat het instelbaar sterk beheerderwachtwoord (voor zowel hard- als software) tenminste acht karakters moet zijn, bestaande uit letters, cijfer(s) en speciale teken(s).

Gezien het specifieke karakter van deze toepassing en de specifieke afspraken rondom de technische realisatie van remote support per Deelnemer kunnen

gelden, dient de Deelnemer hier met de Opdrachtnemer aanvullende afspraken over te maken en deze vast te leggen in een Dossier Afspraken en Procedure (DAP).

3.7 Beveiligingsinstellingen Product

Voor zover een dienst wordt afgenomen waarbij Producten worden afgeleverd inclusief het instellen van beveiligingsinstellingen van het Product, dienen in die gevallen de mogelijke beveiligingsinstellingen van het Product vóór Aflevering tussen Opdrachtnemer en Deelnemer te worden besproken en te worden vastgelegd in de blauwdruk. De afspraken over beveiligingsinstellingen van het Product betreffen onder andere:

- hardening: het uitschakelen en/ of blokkeren van niet gebruikte netwerkpoorten en protocollen;
- toegangsbeheer gebruik: de afspraken voor de wachtwoorden, gebruikersaccounts en de *Simple Network Management Protocol (*SNMP) community names;
- toegangsbeheer fysieke componenten: de afspraken rond het beveiligen van componenten van het Product, waaronder de datadrager en ongebruikte functionaliteiten (bijvoorbeeld de fax functie). Voorkomen van ongeoorloofde toegang tot het component, waaronder het ongeoorloofd kunnen verwijderen of gebruiken;
- voorkomen van ongeoorloofde toegang tot het component, waaronder het ongeoorloofd kunnen verwijderen of gebruiken;
- toegangbeheer interfaces: interfaces (zoals, maar niet uitsluitend, (draadloze) netwerkinterfaces en USB-interfaces) dienen geblokkeerd of verwijderd of uit te schakelen te zijn;
- wijzigingsbeheer: afspraken, waaronder autorisatie, betreffende het uitvoeren van software firmware updates en upgrades op de Producten;
- het uitvoeren van firmware upgrades is alleen mogelijk na autorisatie.

3.8 Infrastructurele beveiligingseisen

Voor alle Producten en Diensten geldt dat de toegang tot de infrastructuur afgesloten moet zijn voor onbevoegden, tenzij dit niet mogelijk is en als zodanig is overeengekomen met de Deelnemer. Onder toegang wordt zowel fysieke als logische toegang verstaan. Ongeautoriseerde toegang dient gedetecteerd te worden, waarna passende maatregelen worden getroffen. De toegangsmethoden tot de Diensten en de te nemen maatregelen bij ongeautoriseerde toegang, dienen in de beveiligingsparagraaf van het Dossier Afspraken en Procedures vastgelegd te worden.
De Opdrachtnemer dient de integriteit[4] en vertrouwelijkheid[5] van het over zijn netwerk getransporteerde gesprek/verkeer van de Deelnemer te waarborgen.

[4] Integriteit: De inhoud van een gesprek/verkeersstroom kan tijdens het transport niet worden gewijzigd.

[5] Vertrouwelijkheid: Onbevoegden kunnen de inhoud van een gesprek/verkeersstroom niet afluisteren,aftappen, kopiëren, etc..

De Opdrachtnemer dient voor alle Producten, Diensten en Gebruiksrechten Professionele maatregelen te nemen om de mogelijkheid van afluisteren van netwerkverbindingen en/of wijzigen van datastromen te verhinderen. Hiertoe worden binnen de branche gebruikelijke maatregelen toegepast. De Opdrachtnemer dient op aanvraag van de Deelnemer inzichtelijk te maken welke maatregelen geïmplementeerd zijn en hoe deze gecontroleerd worden.

3.9 Toegangscontrole

Informatiesystemen betrokken bij de Prestatie moeten zijn ingericht volgens een Professioneel autorisatiemodel. Accounts op informatiesystemen betrokken bij de Prestatie beschikken uitsluitend over toegangsrechten gekoppeld aan rollen toegekend via het vigerende Professionele autorisatieproces. Opdrachtnemer dient aantoonbaar operationeel geborgde Professionele beleidsregels, procedures en beheersmaatregelen te hebben ter bescherming van het informatietransport betrokken bij de Prestatie, dat via alle soorten communicatiefaciliteiten verloopt.

Opdrachtnemer dient beleid te hebben voor functiescheiding (mits redelijkerwijs mogelijk) bij het beleggen van uitvoerende, controlerende, en beheertaken betrokken bij de Prestatie, en dient dit aantoonbaar operationeel geborgd te hebben in processen. Opdrachtnemer dient te beschikken over een operationeel geborgd (project)beheerproces voor de Prestatie waarin informatiebeveiliging aantoonbaar geïntegreerd is.

3.10 Onderhoud en beëindigen Diensten

De Deelnemer kan eisen dat onderhoud van een Dienst, waarop zich gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer bevinden, op de Locatie van de Deelnemer plaatsvindt. De Deelnemer zal de Opdrachtnemer in dit geval adequaat faciliteren.

In het geval van beëindiging dient Opdrachtnemer (delen van) een Dienst, waarop zich gegevens en Programmatuur van de Deelnemer bevinden, nooit zonder voorafgaande toestemming van de Deelnemer en met inachtneming van de optioneel door de Deelnemer gestelde eisen buiten de Locatie te brengen. De Deelnemer kan hierbij aanvullende eisen stellen. De Opdrachtnemer dient een proces-verbaal op te maken.

4 Uitvoeringsaspecten

4.1 Beveiligingsincidenten

Een beveiligingsincident is een gebeurtenis die mogelijk een nadelige invloed heeft op de vertrouwelijkheid, integriteit en/of beschikbaarheid van (bedrijfs-)informatie of (bedrijfs-)informatieverwerkende systemen en derhalve een bedreiging vormt voor de bedrijfsvoering. Iedere activiteit dat het beveiligingsbeleid schendt wordt beschouwd als een beveiligingsincident.

Opdrachtnemer dient over een operationeel geborgd proces te beschikken voor de registratie, rapportage en afhandeling van beveiligingsincidenten die aansluit op het incidentmanagementproces van Opdrachtgever. Periodiek dient over deze beveiligingsincidenten gerapporteerd te worden richting Opdrachtgever. Beveiligingsincidenten dienen onverwijld aan de betreffende functionaris van de Deelnemer te worden gemeld.

4.2 Wijziging in beveiliging

Wijzigingen welke de beveiliging kunnen aantasten worden voorafgaand met de Deelnemer besproken, waarbij de risico's worden benoemd en eventuele maatregelen worden geadviseerd.

4.3 Organiseren van informatiebeveiliging

Opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002. De in de Raamovereenkomst opgenomen proces- en systeemvereisten van Opdrachtgever maken middels een toepasselijkheidsverklaring aantoonbaar onderdeel uit van de scope van deze certificering. De Opdrachtnemer dient op aanvraag van de Deelnemer inzichtelijk te maken welke beveiligingsmaatregelen zijn geïmplementeerd en hoe deze gecontroleerd worden.

Opdrachtnemer dient voor informatiebeveiliging minimaal jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC 27005 te maken en passende maatregelen te treffen. Opdrachtnemer dient aantoonbaar te beschikken over een continuïteitsplan voor het handhaven van de Prestatie in ongunstige situaties, waarin ook de continuïteit van de informatiebeveiliging is gewaarborgd.

Opdrachtnemer dient te beschikken over een aantoonbaar operationeel geborgd proces voor het vernietigen van gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Hoofdopdrachtgever, welke zich bevinden op (delen van) informatiesystemen betrokken bij de Prestatie die tijdens de looptijd van het contract afgevoerd of vervangen worden.

Opdrachtnemer dient te beschikken over een formeel en operationeel geborgd Professioneel proces voor back-up en recovery voor van alle informatiesystemen betrokken bij de Prestatie. Het betreft alle aanwezige gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Hoofdopdrachtgever. Opdrachtnemer dient minimaal dagelijks hiervan van back-ups te maken. Opdrachtnemer past bij de back-ups dezelfde beveiligingsmaatregelen toe die ook gelden voor de informatiesystemen betrokken bij de Prestatie.

Opdrachtnemer dient op verzoek van de Deelnemer een actuele registratie te kunnen overleggen van back-upactiviteiten en de fysieke en logische verblijfplaats van de media. De fysieke en logische toegang tot back-ups is zodanig geregeld dat alleen geautoriseerde personen toegang hebben.

Opdrachtnemer dient het recovery proces dat deel uitmaakt van het back-upproces van alle informatie en Programmatuur in gebruik voor de Prestatie, minimaal jaarlijks te testen en naar Opdrachtgever te communiceren over de uitkomst hiervan.

Gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Hoofdopdrachtgever wordt door Personeel van Opdrachtnemer op geen enkele wijze buiten de bij de Prestatie betrokken informatiesystemen en apparatuur gebracht, tenzij dit nodig is voor het leveren van de Prestatie en aantoonbaar is overeengekomen met de Deelnemer en/of Hoofdopdrachtgever.

Opdrachtnemer dient, in het geval dat het contract tussen beide Partijen wordt beëindigd en gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Hoofdopdrachtgever zich bevinden op informatiesystemen betrokken bij de Prestatie, te assisteren bij de overdracht van deze gegevens naar een (eventuele) nieuwe Opdrachtnemer en na de overeengekomen periode te verwijderen.

5 Bronvermeldingen

Onderstaand zijn de links opgenomen van de documenten en onderwerpen die in deze Bijlage zijn genoemd. De opgegeven links zijn de geldige links op het moment van publiceren van de Aanbesteding.

Voor de meest actuele versie van deze documenten tijdens de contractfase dient contact opgenomen te worden met het Centraal Contractmanagement (CCM).

Document	**Locatie**
Beveiligingsvoorschrift Rijksdienst (BVR)	http://www.earonline.nl/index.php/Beveiligingsvoorschrift_Rijksdienst_(BVR)
Baseline Informatiebeveiliging Overheid (BIO)	https://www.bio-overheid.nl/category/producten/producten/
Voorschrift Informatiebeveiliging Rijksdienst (VIR)	http://www.earonline.nl/index.php/Voorschrift_Informatiebeveiliging_Rijksdienst_(VIR)
Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI)	http://www.earonline.nl/index.php/Besluit_Voorschrift_Informatiebeveiliging_Rijksdienst_Bijzondere_Informatie_(VIRBI)
Algemene Verordening Gegevensbescherming (AVG)	https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving
Wet normalisering rechtspositie ambtenaren (Wnra)	https://wetten.overheid.nl/BWBR0039393/2017-05-10
Identificatieplicht	https://www.Rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/met-welke-identiteitsbewijzen-kan-ik-mij-identificeren
Wet veiligheidsonderzoeken	http://wetten.overheid.nl/BWBR0008277/2015-09-01
Door het NBV goedgekeurde producten	https://www.aivd.nl/onderwerpen/informatiebeveiliging/inhoud/beveiligingsproducten/goedgekeurde-producten
Forum Standaardisatie: Pas Toe of Leg Uit	https://lijsten.forumstandaardisatie.nl/lijsten/open-standaarden?lijst=Pas%20toe%20of%20leg%20uit&status%5B%5D=Opgenomen&pagetitle=pastoeof/
NCSC: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls